

501P0364W00

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されて
る事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
this Office.

願 年 月 日
Date of Application:

2000年 3月14日

願 番 号
Application Number:

特願2000-076373

願 人
Applicant(s):

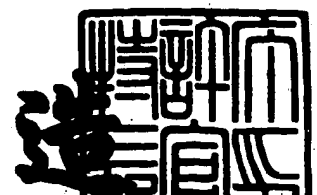
ソニー株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年12月22日

特許庁長官
Commissioner,
Patent Office

及川耕造



【書類名】 特許願

【整理番号】 0000030705

【提出日】 平成12年 3月14日

【あて先】 特許庁長官殿

【国際特許分類】 H04K 1/00

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

 【氏名】 市村 元

【特許出願人】

 【識別番号】 000002185

 【氏名又は名称】 ソニー株式会社

 【代表者】 出井 伸之

【代理人】

 【識別番号】 100086841

 【弁理士】

 【氏名又は名称】 脇 篤夫

【手数料の表示】

 【予納台帳番号】 014650

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

 【包括委任状番号】 9710074

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ送出装置、データ復号装置、データ送出方法、データ復号方法、伝送システム

【特許請求の範囲】

【請求項 1】 デジタルデータをパケット化して送出するデータ送出装置において、

送出するパケットデータの一部に乱数データを挿入する挿入手段と、

上記挿入手段により乱数データが挿入されたパケットデータに対して暗号化処理を行う暗号化手段と、

上記暗号化手段により暗号化されたパケットデータを送出する送出手段と、

を備えたことを特徴とするデータ送出装置。

【請求項 2】 上記送出手段は、有線又は無線で接続された他の機器に対して上記パケットデータを送出することを特徴とする請求項 1 に記載のデータ送出装置。

【請求項 3】 上記送出手段は、上記パケットデータを記録媒体に記録するデータとして送出することを特徴とする請求項 1 に記載のデータ送出装置。

【請求項 4】 上記挿入手段は、パケットデータ内に存在する無効データ部分に、上記乱数データを挿入することを特徴とする請求項 1 に記載のデータ送出装置。

【請求項 5】 送出されてきたパケット化されたデジタルデータを入力する入力手段と、

上記入力手段により入力されたパケットデータに対して暗号化を解読する復号処理を行う復号手段と、

上記復号手段で復号されたパケットデータから乱数データが挿入されたデータ部分を除去する除去手段と、

を備えたことを特徴とするデータ復号装置。

【請求項 6】 上記入力手段は、有線又は無線で接続された他の機器から送出されてきたパケットデータを入力することを特徴とする請求項 5 に記載のデータ復号装置。

【請求項 7】 上記入力手段は、記録媒体から読み出されて送出されてきたパケットデータを入力することを特徴とする請求項 5 に記載のデータ復号装置。

【請求項 8】 上記除去手段は、パケットデータ内に存在する無効データ部分を除去することで、乱数データが挿入されたデータ部分の除去を行うことを特徴とする請求項 5 に記載のデータ復号装置。

【請求項 9】 パケット化されたデジタルデータに対して、パケットデータの一部に乱数データを挿入し、

乱数データが挿入されたパケットデータに対して暗号化処理を行ない、

暗号化されたパケットデータを送出することを特徴とするデータ送出方法。

【請求項 1 0】 送出されてきたパケット化されたデジタルデータを入力し

入力されたパケットデータに対して暗号化を解読する復号処理を行ない、

復号されたパケットデータから乱数データが挿入されたデータ部分を除去することを特徴とするデータ復号方法。

【請求項 1 1】 デジタルデータをパケット化して送出するデータ送出装置と、送出されてきたパケット化されたデジタルデータを復号する復号装置から成る伝送システムにおいて、

上記データ送出装置は、

送出するパケットデータの一部に乱数データを挿入する挿入手段と、

上記挿入手段により乱数データが挿入されたパケットデータに対して暗号化処理を行う暗号化手段と、

上記暗号化手段により暗号化されたパケットデータを送出する送出手段と、

を備え、

上記データ復号装置は、

送出されてきたパケット化されたデジタルデータを入力する入力手段と、

上記入力手段により入力されたパケットデータに対して暗号化を解読する復号処理を行う復号手段と、

上記復号手段で復号されたパケットデータから乱数データが挿入されたデータ部分を除去する除去手段と、

を備えたことを特徴とする伝送システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は暗号化されたパケットデータの伝送を行う伝送システム、及びパケットデータの伝送にかかるデータ送出装置、データ復号装置、データ送出方法、データ復号方法に関するものである。

【0002】

【従来の技術】

例えば著作権保護が必要なデータ、秘密性の高いデータ、プライバシーにかかる私的データなど、外部に漏洩することが好ましくないデータの伝送に際しては、暗号化処理が行われることが多い。

例えば図6に或る送信装置101から受信装置102に対してデータを暗号化して伝送するモデルを示す。

【0003】

いま、伝送しようとするデータDTが送信装置101に入力されたとすると、送信装置101は、まず暗号化部111で暗号化処理を施し、暗号化されたデータDTsを生成する。

そしてそのデータDTsは送信部112から送信出力される。

送信出力されたデータDTsは例えばIEEE1394バスなどの伝送路103により、受信装置102に送られることになる。

受信装置102では、伝送路103から送信されてきたデータDTsを受信部121で受信し、復号部122で暗号解読処理を行うことで、元のデータDTを得ることができる。

【0004】

【発明が解決しようとする課題】

このように伝送路103においては暗号化されたデータDTsが送信されることで、仮に伝送路103においてデータDTsが取り出されたとしても、データDTの内容は秘密性が保たれるものとなる。

しかしながら、例えば著作権保護を目的として音楽データ等を図6のようなシステムで伝送する場合、暗号を解読され、結果として違法なコピーが行われるおそれがある。

【0005】

例えば伝送しようとするデータDTがPCMオーディオデータであったとする。

PCMオーディオデータの場合、無音部分、例えば曲と曲の間の期間に相当する部分や、再生装置等でアクセスが行われて、データとしてミュートパターンが配されている部分などでは、データストリーム上でゼロデータが並んでいるものとなっている。又は例えば $\Delta\Sigma$ 変調された1ビットオーディオデータの場合、無音部分は「96h」(=10010110)などの固定パターンとなっている。

ここで、破線で示すように、何らかの手段で伝送路103から暗号化されたデータDTsが取り出されたとする。

通常は、データDTsを解析しても、元のデータDT自体がわからないため、暗号の解読は困難である。

ところが、データDTsにおいて、データDTの無音部分に相当する部分を抽出されると、元のデータがゼロデータ等の固定パターンであること、つまり元のデータの内容が明白となっていることから、比較的容易に暗号が解読され、データDTの内容や暗号化アルゴリズムが知られてしまう危険性がある。

もちろん暗号化アルゴリズムが解読されれば、悪意のユーザーによればその後データDTの違法な取り込みが容易に可能となってしまう。つまり著作権侵害となるような行為を実行可能としてしまう。

【0006】

従って、音楽データ等の著作権保護が必要なデータについて、機器間の伝送、記録媒体への記録のための伝送、或いは公衆回線等を用いた音楽配信システムにおける伝送などの広範囲の分野で、上記の危険性が内包されており、このため違法な暗号解読を防止できるような技術が求められている。

【 0 0 0 7 】

【課題を解決するための手段】

本発明はこのような状況に鑑みて、伝送されるデータについて、容易に暗号解読ができないようにする技術を提供するものである。

【 0 0 0 8 】

このため本発明では、デジタルデータをパケット化して送出するデータ送出装置として、送出するパケットデータの一部に乱数データを挿入する挿入手段と、上記挿入手段により乱数データが挿入されたパケットデータに対して暗号化処理を行う暗号化手段と、上記暗号化手段により暗号化されたパケットデータを送出する送出手段と、を備えるようにする。

例えば上記挿入手段は、パケットデータ内に存在する無効データ部分に、上記乱数データを挿入する。

また本発明のデータ復号装置は、送出されてきたパケット化されたデジタルデータを入力する入力手段と、上記入力手段により入力されたパケットデータに対して暗号化を解読する復号処理を行う復号手段と、上記復号手段で復号されたパケットデータから乱数データが挿入されたデータ部分を除去する除去手段と、を備えるようにする。

例えば上記除去手段は、パケットデータ内に存在する無効データ部分を除去することで、乱数データが挿入されたデータ部分の除去を行う。

また、本発明の伝送システムは、上記構成のデータ送出装置と上記構成のデータ復号装置により構成されるものとする。

そしてデータ送出装置とデータ復号装置は、それぞれ異なる機器間における送信装置、受信装置としたり、記録媒体に記録を行う記録装置における記録データの送出装置、記録媒体からデータの再生を行う再生装置における再生データの復号装置などとして実現されるようにする。

【 0 0 0 9 】

また本発明のデータ送出方法は、パケット化されたデジタルデータに対して、パケットデータの一部に乱数データを挿入し、乱数データが挿入されたパケットデータに対して暗号化処理を行ない、暗号化されたパケットデータを送出するも

のとする。

本発明のデータ復号方法は、送出されてきたパケット化されたデジタルデータを入力し、入力されたパケットデータに対して暗号化を解読する復号処理を行ない、復号されたパケットデータから乱数データが挿入されたデータ部分を除去するようにする。

【 0 0 1 0 】

即ち本発明では、暗号化を行う前にパケットデータ内に乱数データを挿入する。これによって、例えば元のデータにおいてゼロデータ列などの内容が明確な部分が存在しても、その部分が不明確な状態となるようにした上で暗号化されることとなるため、暗号アルゴリズムの解読は非常に困難なものとなる。

【 0 0 1 1 】

【発明の実施の形態】

以下、本発明の実施の形態を次の順に説明する。

1. 送信装置及び受信装置に本発明を採用する例
2. I E E E 1 3 9 4 でオーディオパケットデータを伝送する場合の乱数データ挿入例
3. 記録装置及び再生装置に本発明を採用する例

【 0 0 1 2 】

1. 送信装置及び受信装置に本発明を採用する例

本発明のデータ送出装置（データ送出方法）、データ復号装置（データ復号方法）を、送信装置、受信装置に採用する実施の形態を説明する。

図 1 は、或る 2 つの機器が例えば I E E E 1 3 9 4 バスによる伝送路 3 により接続されている場合に、送信装置 1 を有する機器から受信装置 2 を有する機器にデータ D T を伝送するモデルにおいて本発明の実施の形態を示したものである。

パケット構造については後述するが、データ D T は、例えば 1 ビットデジタル

オーディオデータを、所定の伝送プロトコルに合致するフォーマットに基づいてパケット化（ブロック化）したものであるとする。

【 0 0 1 3 】

1ビットデジタルオーディオデータとは、通常のCD（Compact Disc）におけるオーディオデータよりも高品位なデータとして開発されたものであり、サンプリング周波数を例えばCD方式における44.1kHzの16倍という非常に高いサンプリング周波数である2.842MHzとして $\Delta\Sigma$ 変調された1ビットデータのことであり、周波数帯域はDC成分～100kHzの広範囲とされ、ダイナミックレンジはオーディオ帯域全体で120（dB）を実現できるデータ形式である。

なお、本例ではこのような1ビットデジタルオーディオデータをパケット化して伝送する場合を例に挙げるが、もちろん伝送されるデータ自体の形式、種別はどのようなものでもよい。

【 0 0 1 4 】

図示するように送信装置1は、ランダムデータ付加部11、暗号化部12、送信部13が設けられる。

ランダムデータ付加部11は内部に乱数発生回路を備え、送信しようとするデータDT（パケットデータ）の所要の部分に乱数発生回路で発生させた乱数データを付加する動作を行う。

暗号化部12は、ランダムデータ付加部11の出力に対して所定の暗号アルゴリズムでの暗号化処理を施す。

送信部13は暗号化部12の出力をIEEE1394バスによる伝送路3に送出する動作を行う。

【 0 0 1 5 】

受信装置1は、受信部21、復号部22、ランダムデータ除去部23を備える。

受信部21は、伝送路3から供給されるデータを受信して取り込む動作を行う。

復号部22は、上記暗号化部12での暗号化アルゴリズムに対応して暗号解読

処理を行う部位である。

ランダムデータ除去部 2 3 は、上記ランダムデータ付加部 1 1 で付加された乱数データ部分を除去する部位である。

【 0 0 1 6 】

このような送信装置 1、受信装置 2 においてデータ D T の伝送は次のように行われる。

パケットデータとして伝送しようとするデータ D T が送信装置 1 に入力されたとすると、送信装置 1 は、まずランダムデータ付加部 1 1 で、パケット内の所定の部位に乱数データを挿入する。具体例は後述するが、パケットデータ内の無効データ部分に乱数データを挿入することになる。

ランダムデータ付加部 1 1 で乱数データが挿入されたデータ D T a d は、続いて暗号化部 1 2 に供給され、暗号化処理が施される。

暗号化されたデータ D T s は、送信部 1 3 に供給され、送信部 1 3 から伝送路 3 に対して送出されることになる。

【 0 0 1 7 】

このように送信されたデータ D T s を受信する受信装置 2 では、まず伝送路 3 から供給されてきたデータ D T s を受信部 2 1 で受信し、復号部 2 2 に供給する。復号部ではデータ D T s に対する暗号解読処理を行うことで、暗号化前のデータ、即ち乱数データが付加されている状態のデータ D T a d が出力される。

このデータ D T a d はランダムデータ除去部 2 3 に供給され、ランダムデータ部分が除去されることで、当初の送信データ、即ちデータ D T が得られることとなる。

【 0 0 1 8 】

ここで破線で示すように、何らかの手段で伝送路 3 から暗号化されたデータ D T s が取り出された場合を考える。

上述したようにデータ D T s において元の内容が明白な部分（無音部分）が抽出されると暗号化アルゴリズムが解読されるおそれがある。

しかしながら本例の場合、データ D T s は、乱数データが付加された上で暗号化されたものである。つまりゼロデータ等の固定パターンが連続する部分がなく

された状態で暗号化されている。従ってデータDTsから、無音部分に相当するデータ部分を抽出することは困難となり、この点で暗号解読は困難となる。

また、仮にデータDTsにおいて、元の1ビットデジタルオーディオデータとしての無音部分、即ちゼロデータが連続している部分に相当する部分が抽出され、データDT（つまりゼロデータ）とDTsが比較解析されたとする。

ところがこの場合でも、データDTsは、乱数データを含めた上で暗号化されているため、データDTsの解析処理において、データDTs上では暗号化アルゴリズムによるデータ要素と乱数データによるデータ要素を区別することはできず、従って、暗号化アルゴリズムを解析することはほぼ不可能である。

【0019】

以上のことから、本例によれば伝送路3で伝送されるデータについて暗号解読は非常に困難なものとなり、従って、著作権保護を要するデータの伝送などに非常に好適なものとなる。

また送信装置1側では従前の構成にランダムデータ付加部11を設けるだけでよく、受信装置2側では、ランダムデータ除去部23を設けて、暗号化を解読したうえで乱数データが挿入されたデータ部分を除去するのみでデータを復号できる。従って送信装置1、受信装置2としての構成がさほど複雑化することもなく、各種の機器への導入は容易なものとなる。

【0020】

2. IEEE1394でオーディオパケットデータを伝送する場合の乱数データ挿入例

ここで、例えば図1の伝送システムにおいてデータDTに乱数データを付加する場合の態様について説明する。

【0021】

図2は送信しようとするデータDTとしてのデータパケット構造例を示している。

この図2の packets 構造は、IEEE 1394 バスによるデータ伝送について適用できる AM824 と呼ばれる伝送プロトコルに基づいた例であり、その場合において1ビットデジタルオーディオデータとして6チャンネルのオーディオデータを伝送する場合の packets 構造例を示している。

【0022】

32ビット（4バイト）を1カドレット（Quadlet）と呼ぶとすると、6チャンネルデータの場合、8カドレット（q1～q8）で1つの packets（ブロック）が形成され、この packets が連続するものとなる。

1568 packets の範囲が1フレームと呼ばれる単位となる。

そして1ビットデジタルオーディオデータとしての伝送データストリームは、このようなフレームが連続されて形成される。

【0023】

カドレットにおける先頭のバイト（バイト0）は、ラベルとされている。ラベルとは、そのカドレットに配されるデータの識別情報となる。

ラベルとしての値及び意味を図3に示す。

図示するようにラベル値に対して各種の意味が定義されており、例えばラベル値40h～4Fhは、DVD（Digital Versatile Disc）システムで採用されているマルチビットリニアオーディオデータに対応するものとされる。なお、「h」を付した数値は16進表記のものである。

またラベル値50h～57hは、1ビットデジタルオーディオデータに対応する値、ラベル値58h～5Fhは、エンコードされた1ビットデジタルオーディオデータに対応する値、ラベル値80h～83hはMIDIデータに対応する値とされる。

さらにC0h～EFhはアンシラリーデータ（Ancillary Data；補助データ）を意味するなど、ラベル値は識別情報として機能するために各種定義されている。

【0024】

各ラベル値についての詳細な定義の説明は本発明と直接関係がないため説明を省略するが、図2に示した値についてのみ述べると次のようになる。

【0025】

図2においてパケット#0の第1カドレットq1をみると、ラベル値は「D1h」とされている。従って第1カドレットq1はアンシラリデータが記述されるものと提示されていることになり、さらにこの場合バイト1はサブラベルとされて「00h」とされている。

このときバイト2、バイト3が実際の補助データ内容となるが、ここではコピーコントロール情報、チャンネル数、スピーカ配置情報が記述される。

【0026】

第2カドレットq2ではラベル値は「50h」とされる。ラベル値50h～57hは、1ビットデジタルオーディオデータに対応する値であるが、「50h」は、マルチチャンネルのデータを配したブロックの最初のデータであることを示す。

また第3～第7カドレット(q3～q7)ではラベル値は「51h」とされる。「51h」は、マルチチャンネルのデータを配したブロックの2番目以降のデータであることを示す。

従って、第2～第7カドレット(q1～q7)では、チャンネル1～チャンネル6の6チャンネルの1ビットデジタルオーディオデータが配されていることが示されるものとなる。各チャンネルのデータはバイト1～バイト3の3バイトで記述される。

【0027】

第8カドレットq8では、ラベル値は「CFh」とされている。これはアンシラリデータの範疇であるが、「CFh」は特に無効データ(NO DATA)を示す値として定義されている。

またこの場合は、バイト1は無効データの内容を示す値とされており、この例のような「50h」は1ビットデジタルオーディオデータとしての無効データを示すものとなる。

そしてこのときバイト2、バイト3が無効データにより充填される。

【0028】

パケット#1の第1カドレットq1では、ラベル値は「D1h」とされている

。従って第1カドレットq1はアンシラリデータが記述されるものと提示されていることになり、さらにこの場合バイト1はサブラベルとされて「01h」とされている。

このときはバイト2、バイト3の補助データ内容は、サブリメンタリデータとされる。

第2～第8カドレットはパケット#0と同様である。

【0029】

パケット#1567の第1カドレットq1では、ラベル値は「CFh」とされている。つまりバイト2、バイト3は無効データである。ただし、バイト1は「D1h」とされていることで、アンシラリデータとしての無効データであることが示されている。

第2～第8カドレットはパケット#0と同様である。

【0030】

例えばこのようなパケットデータストリームを伝送する場合を例に挙げると、上述した送信装置1のランダムデータ付加部11では、無効データの部分に乱数データを挿入すればよい。

即ち各パケットにおいて斜線部を付した無効データ部分に乱数データを挿入する。具体的にはランダムデータ付加部11では1パケットあたりに2バイトの乱数データを生成し、無効データのカドレット、つまりラベル値＝「CFh」のカドレットのバイト2、3の2バイトに挿入するものである。

このように乱数データを挿入することにより、パケット内のオーディオデータが仮にオールゼロ、あるいは「96h」などの固定パターンであったとしても、オールゼロあるいは「96h」等とは見えないものとなり、上述の通り、暗号解読を防止できるものとなる。

【0031】

また、このように無効データ部分に乱数データを挿入することは、受信装置2側での処理が非常に簡単となることを意味する。

即ち受信装置102の復号部22で暗号解読処理が施されると、図2の状態のパケットデータストリームがランダムデータ除去部23に供給されることになる

が、ランダムデータ除去部 2 3 では、ラベル値 = 「C F h」のカドレットを捨てればよいのみとなる。

ラベル値 = 「C F h」のカドレットは無効データとして本来捨てられるものであるため、その意味でいえば、ランダムデータ除去部 2 3 は何ら特別な処理を必要としないものともなる。

【 0 0 3 2 】

3. 記録装置及び再生装置に本発明を採用する例

続いて、本発明のデータ送出装置（データ送出方法）、データ復号装置（データ復号方法）を、記録装置、再生装置に採用する実施の形態を説明する。

記録装置は記録媒体に対するデータ送出装置となり、また再生装置は記録媒体から読み出されたデータのデータ復号装置となる。

【 0 0 3 3 】

図 4 は所定の記録媒体（メディア）6 に対してデータ D T を記録できる記録装置である。

図示するように記録装置 4 は、入力されてくるデータ D T に対する記録処理系として、暗号化部 4 0，エンコード及び記録ドライブ部 4 4、記録ヘッド（又はインターフェース）4 5 が設けられる。

暗号化部 4 0 は、ランダムデータ付加部 4 1，暗号化部 4 2、送出部 4 3 を有する。

【 0 0 3 4 】

このような記録装置 4 では、入力されたデータ D T について、ランダムデータ付加部 4 1 は内部に乱数発生回路から発生させた乱数データを、データ D T の所要の部分に付加する。

ランダムデータ付加部 4 1 で乱数データが挿入されたデータ D T a d は、続いて暗号化部 4 2 に供給され、暗号化処理が施される。

暗号化されたデータ D T s は、送出部 4 3 に供給され、送出部 4 3 からエンコ

ード及び記録ドライブ部 4 4 に送出される。

エンコード及び記録ドライブ部 4 4 は、供給されたデータ D T s に対して、記録を行うメディア 6 の記録フォーマット、変調方式に応じてエラー訂正符号の付加や各種エンコード処理を行い、記録ドライブ信号を生成する。

その記録ドライブ信号は記録ヘッド 4 5 に供給されて記録ヘッド 4 5 によりメディア 6 へのデータ書込が行われる。

例えばメディア 6 が光ディスク、光磁気ディスク、磁気ディスク、磁気テープなどであれば、記録ドライブ信号に応じて光学ヘッド又は磁気ヘッドが駆動されて記録が実行される。

また、メディア 6 がフラッシュメモリなどによるメモリカードのような形態であれば、インターフェース 4 5 によりメディア 6 に対して書込アクセスが行われることになる。

【 0 0 3 5 】

図 5 はは所定の記録媒体（メディア） 6 からデータ D T を再生できる再生装置である。

図示するように再生装置 5 は、メディア 6 からデータの読み出しを行う再生ヘッド（又はインターフェース） 5 4、デコード部 5 5、復号部 5 0 が設けられる。

復号部 5 0 は、取込部 5 1、復号部 5 2、ランダムデータ除去部 5 3 を備える。

【 0 0 3 6 】

この再生装置 5 では、例えばメディア 6 としての光ディスク、光磁気ディスク、磁気ディスク、磁気テープなどから光学ヘッド又は磁気ヘッドとしての再生ヘッド 5 4 によって読み出されたデータ、或いはメディア 6 としてのメモリカードからインターフェース 5 4 を介した読出アクセスにより読み出されたデータは、デコード部 5 5 で、メディア 6 の記録フォーマットに応じたデコード処理やエラー訂正処理が行われる。そしてそのデコードされたデータは、即ち記録装置 4 で暗号化されたデータ D T s であり、データ D T s は取込部 5 1 により復号部 5 0 内に取り込まれ、復号部 5 2 で暗号解読処理される。

復号部 5 2 で、上記暗号化部 4 2 での暗号化アルゴリズムに対応した暗号解読処理を行うことで、ランダムデータが付加された状態のデータ D T a d とされる。そして、そのデータ D T a d がランダムデータ除去部 5 3 に供給されて、上記ランダムデータ付加部 4 1 で付加された乱数データ部分が除去されることで、元のデータ D T が再生されるものとなる。

【 0 0 3 7 】

記録装置 4、再生装置 5 が以上のように構成されることで、メディア 6 に記録されるデータは、乱数データが付加された上で暗号化されたデータ D T s がエンコードされたものである。つまり例えば元のオーディオデータとしてゼロデータが連続する部分があったとしても、そのゼロデータ等の固定パターンが連続する部分がなくされた状態で暗号化されたデータがエンコードされている。

従ってメディア 6 に記録されたデータをデコードしても、無音部分に相当するデータ部分を抽出することは困難となり、この点で暗号解読は困難となる。

さらにゼロデータが連続している部分に相当する部分が抽出され、データ D T (つまりゼロデータ) と D T s が比較解析されたとしても、データ D T s は、乱数データを含めた上で暗号化されているため、データ D T s の解析処理において、データ D T s 上では暗号化アルゴリズムによるデータ要素と乱数データによるデータ要素を区別することはできず、従って、暗号化アルゴリズムを解析することはほぼ不可能である。

【 0 0 3 8 】

つまりこのような記録装置、再生装置によれば、メディア 6 に記録されるデータについて暗号解読は非常に困難なものとなり、従って、著作権保護を要するデータの記録などに非常に好適なものとなる。また、上述した送信装置 1、受信装置 2 の場合と同様に、記録装置 4、再生装置 5 として構成がさほど複雑化することもなく、導入は容易である。

【 0 0 3 9 】

なお、図 4、図 5 として記録装置 4、再生装置 5 を分けて示したが、これらの回路構成を 1 つの機器に設けて、記録再生装置とすることはもちろん可能である。

また、記録装置 4（又は記録再生装置）としては、必ずしも暗号化部 40 を設けなくてもよい。例えば伝送路 3 を介して或る送信装置から伝送されてきたデータを記録する記録装置を考えると、その送信装置側が図 1 に示した構成を備えていれば、記録装置に伝送されてくるデータは、既に乱数データが付加された上で暗号化されたデータ D T s となっている。従ってその場合、記録装置は暗号化部 40 は不要となる。そして再生装置は、図 5 に示した復号部 50 を備えることで、伝送され記録されたデータの再生を行うことができるようになる。

例えば音楽等の配信システムなどを想定すると、このような形態が好適なものとなる。

【 0 0 4 0 】

以上、実施の形態を説明してきたが、本発明はさらに多様な構成例が考えられ、また送信装置、受信装置、記録装置、再生装置などの形態で多種多様な機器に導入できるものである。

また、上記例では送信装置 1 と受信装置 2 は有線としての I E E E 1 3 9 4 方式の伝送路 3 による伝送システムとしたが、他の伝送規格によるものでもよく、また衛星通信、無線電話通信、赤外線伝送などの無線伝送システムに本発明を適用できることはもちろんである。

また、伝送するデータは図 2 に示したようなパケットデータに限定されるものではなく、あらゆるデータの伝送に本発明を適用できる。特に本発明でいう「パケット」とは広い意味であり、一般に「ブロック」「フレーム」「セクター」「クラスタ」などと呼ばれる各種データ単位を含むものである。

【 0 0 4 1 】

【発明の効果】

以上の説明からわかるように、本発明によれば、伝送するデータについて、パケットデータ内に乱数データを挿入したうえで暗号化を行なって伝送するようにしている。このため、例えば元のデータにおいてゼロデータ列などの内容が明確な部分が存在しても、その部分が不明確な状態となるようにした上で暗号化されることとなるため、伝送過程などで暗号化データが抽出されたとしても、暗号アルゴリズムの解読は非常に困難なものとなるという効果があり、従って著作権保

護などに好適なものとなる。

また、このように乱数データが付加された上で暗号化されたデータを復号する場合は、暗号化を解読したうえで乱数データが挿入されたデータ部分を除去するのみでデータを復号できるため、復号のために複雑な処理は必要なく、簡易な構成で復号装置を実現できる。

換言すれば本発明では、データ送出装置、データ復号装置としては装置構成の複雑化を招かずに、暗号解読が非常に困難なデータ伝送を実現できるものとなる。

【 0 0 4 2 】

また本発明では、データ送出装置側では、パケットデータ内に存在する無効データ部分に乱数データを挿入することで、パケットとしての構造を保ったまま本発明の効果を實現でき、伝送方式やパケット仕様の変更やそれに伴う処理の変更なども不要であるため、従前の伝送システムなどに容易に導入できる。

またその場合、データ復号装置側では、パケットデータ内に存在する無効データ部分を除去するというのみで、乱数データが挿入されたデータ部分の除去を行うことができるため処理は非常に容易なものとなる。

【 0 0 4 3 】

またデータ送出装置とデータ復号装置は、それぞれ異なる機器間における送信装置、受信装置とすることで、機器間のデータ伝送において上記効果を實現できる。

さらにデータ送出装置とデータ復号装置は、それぞれ記録媒体に記録を行う記録装置における記録データの送出装置、記録媒体からデータの再生を行う再生装置における再生データの復号装置とすることで、記録媒体に記録されているデータ、又は記録再生の過程のデータにおいて上記効果を實現できる。

【図面の簡単な説明】

【図 1】

本発明の実施の形態の送信装置及び受信装置のブロック図である。

【図 2】

実施の形態のパケットデータの説明図である。

【図3】

実施の形態のパケットデータのラベルの説明図である。

【図4】

実施の形態の記録装置のブロック図である。

【図5】

実施の形態の再生装置のブロック図である。

【図6】

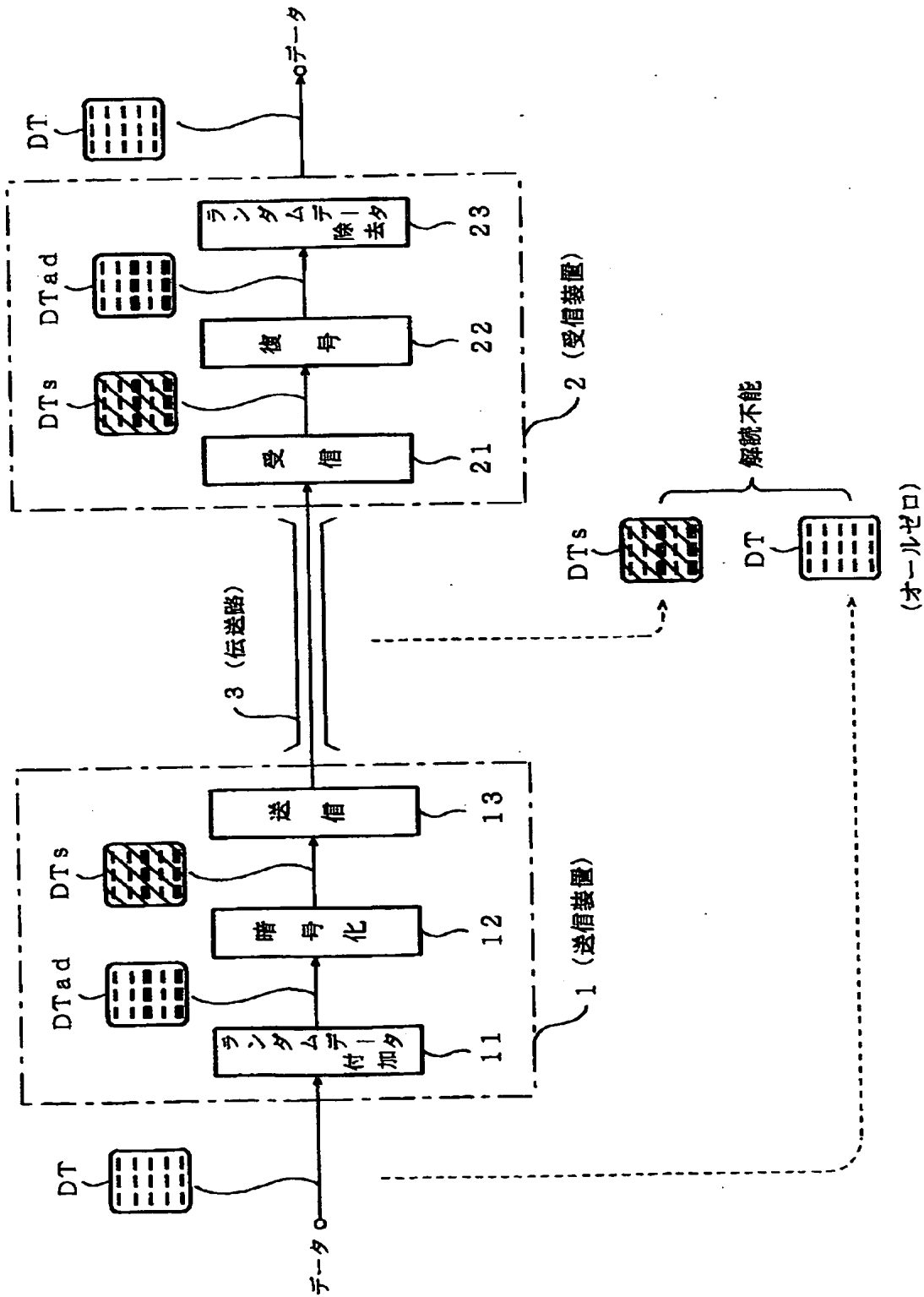
従来の伝送システムの説明図である。

【符号の説明】

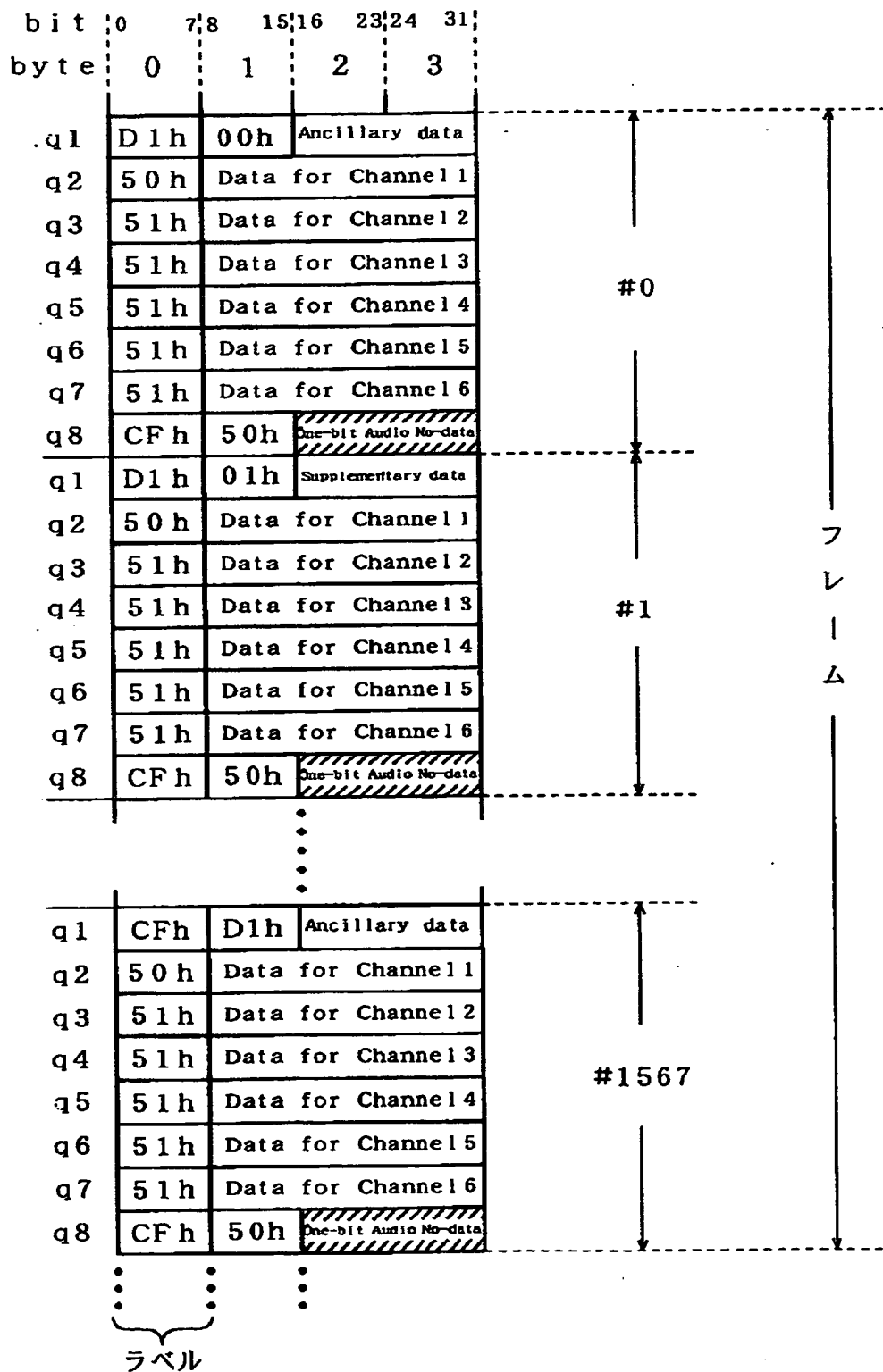
1 送信装置、2 受信装置、3 伝送路、4 記録装置、5 再生装置、6
メディア、11, 41 ランダムデータ付加部、12, 42 暗号化部、13
送信部、21 受信部、22, 52 復号部、23, 53 ランダムデータ除
去部、43 送出部、51 取込部

【書類名】 図面

【図1】



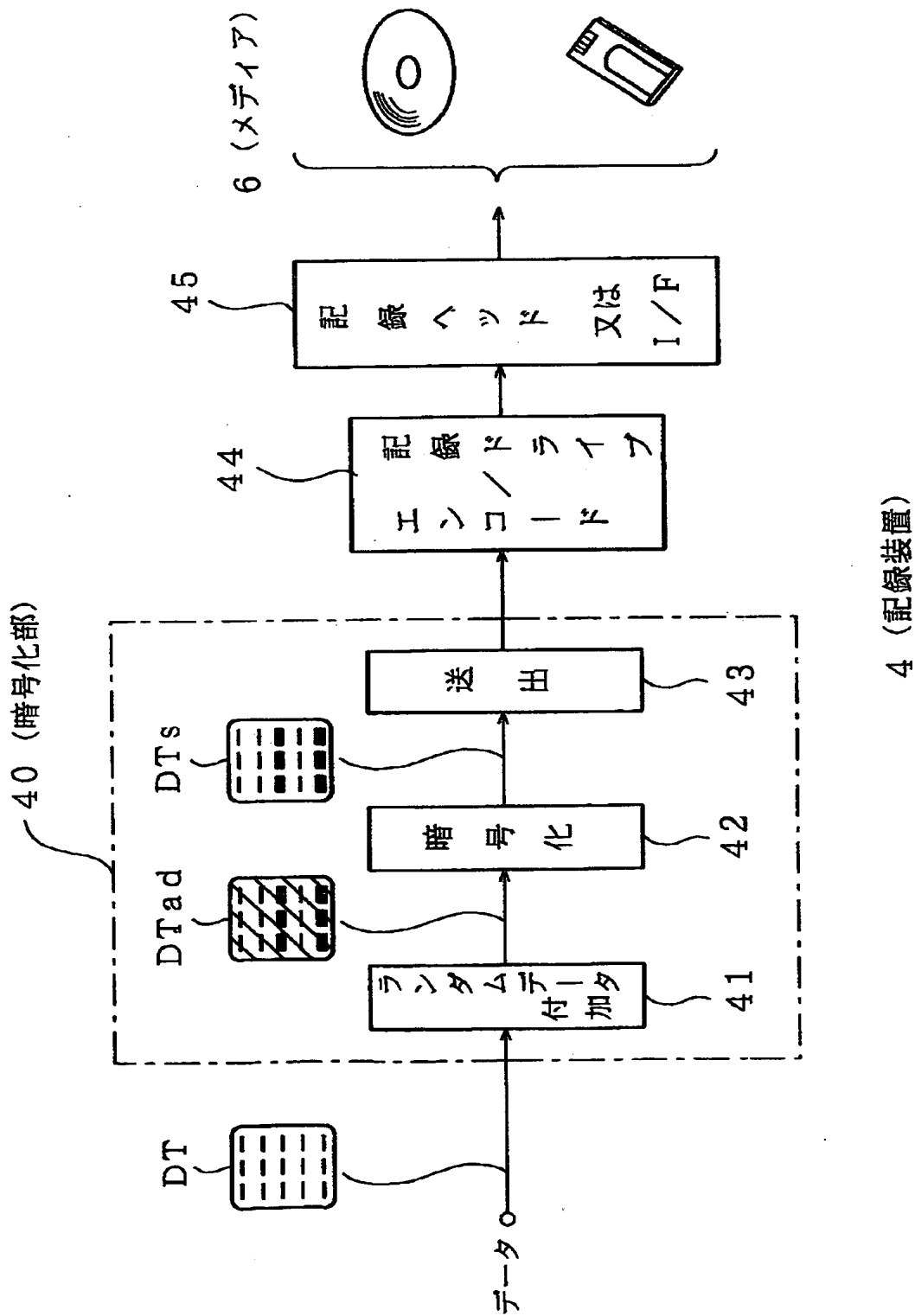
【図2】



【図3】

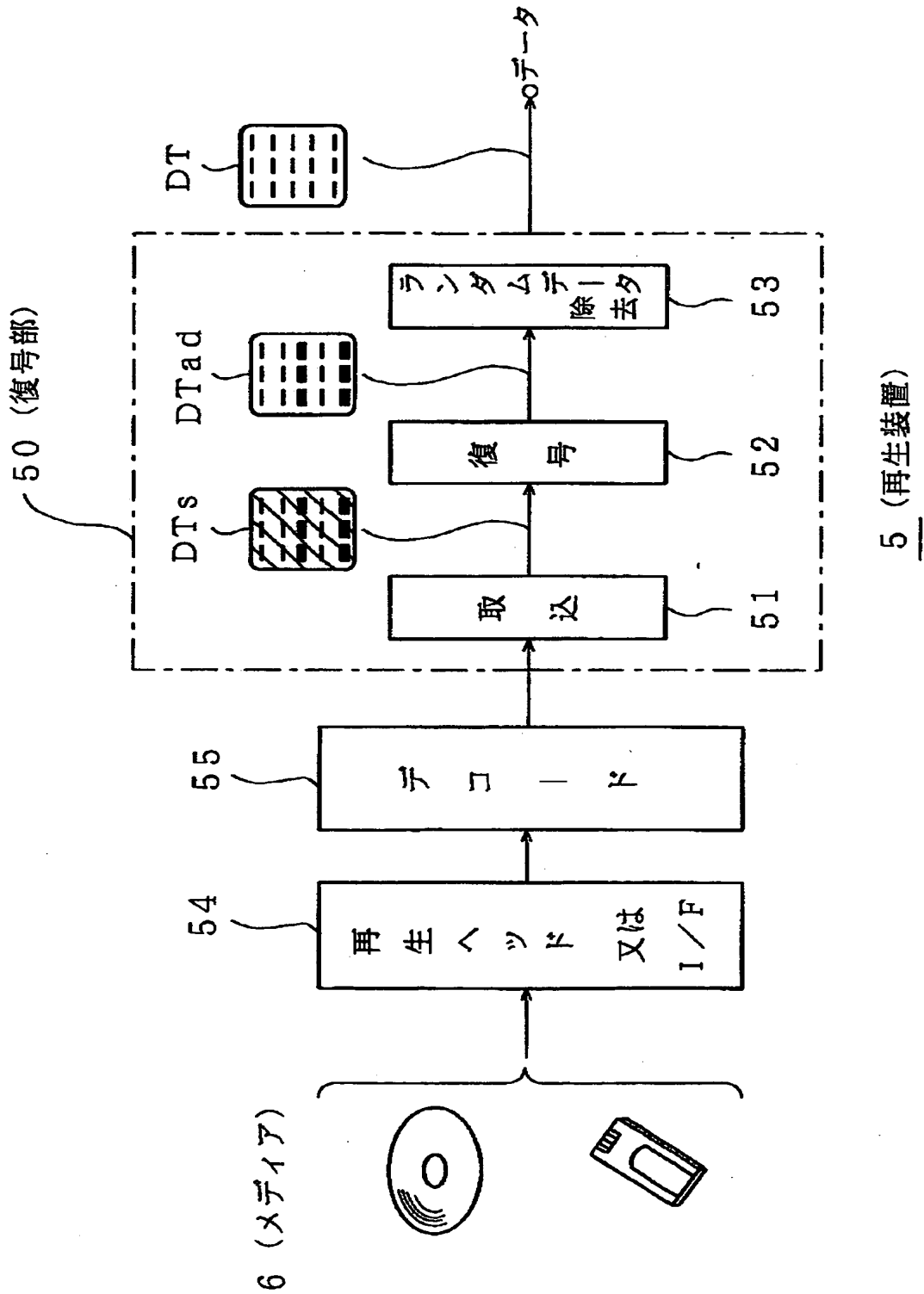
| Value | Description |
|---------|----------------------------|
| 00h-3Fh | IEC60958 Conformant |
| 40h-4Fh | Multi-bit Linear Audio |
| 50h-57h | One Bit Audio (Plain) |
| 58h-5Fh | One Bit Audio (Encoded) |
| 60h-7Fh | -reserved- |
| 80h-83h | MIDI Conformant |
| 84h-87h | Extended Music Data |
| 88h-8Bh | SMPTE Time Code Conformant |
| 8Ch-8Fh | Sample Count |
| 90h-BFh | -reserved- |
| C0h-EFh | Ancillary Data |
| F0h-FFh | -reserved- |

【図4】

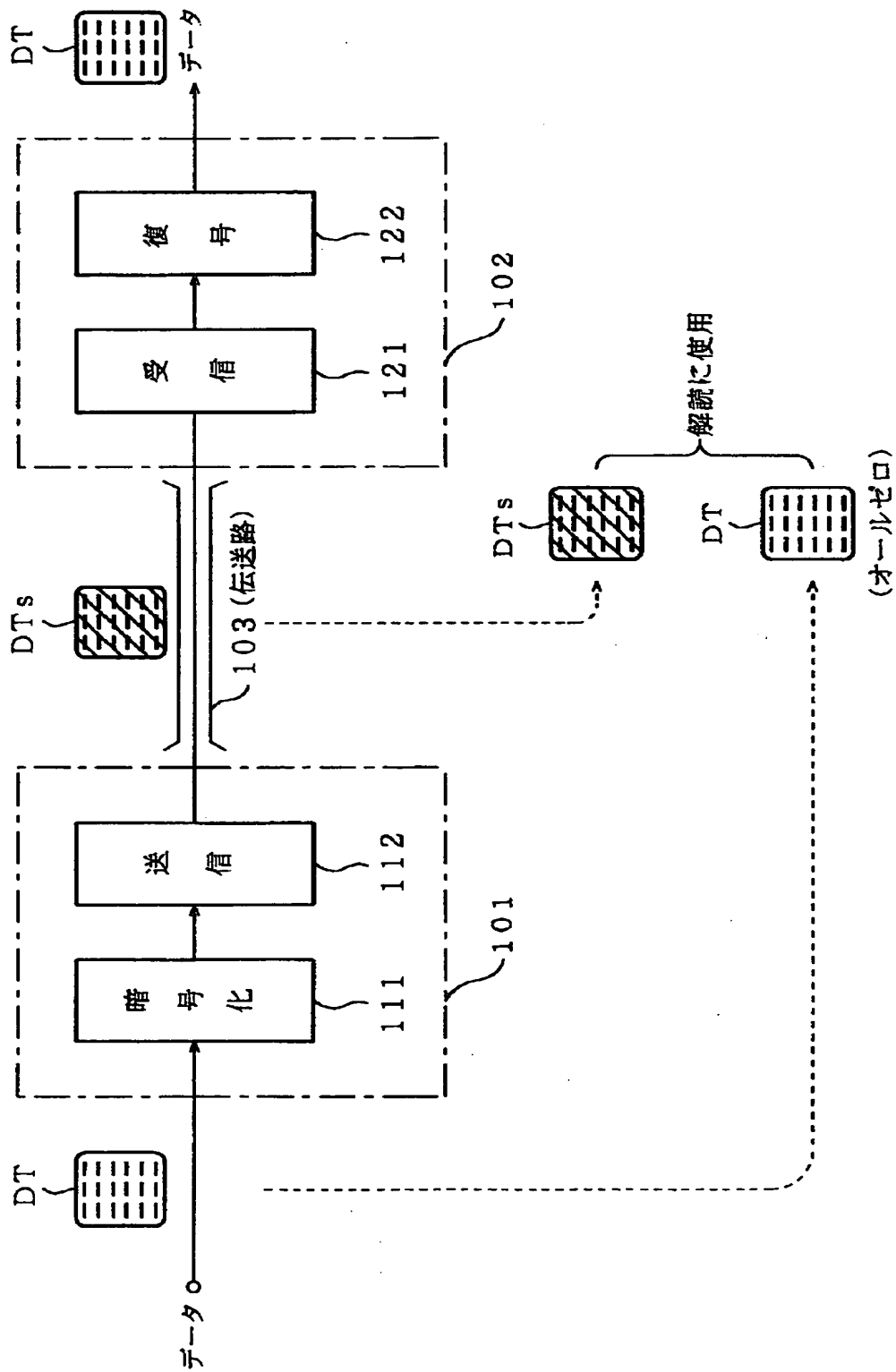


4 (記録装置)

【図 5】



【図6】



【書類名】 要約書

【要約】

【課題】 暗号解読が困難で著作権保護などに好適なデータ伝送の実現。

【解決手段】 伝送するデータについて、パケットデータ内に乱数データを挿入したうえで暗号化を行なって伝送し、伝送過程などで暗号化データが抽出されたとしても、暗号アルゴリズムの解読を困難なものとする。データの復号は、暗号化を解読したうえで乱数データが挿入されたデータ部分を除去することで行う。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000002185]

| | |
|----------|-------------------|
| 1. 変更年月日 | 1990年 8月30日 |
| [変更理由] | 新規登録 |
| 住 所 | 東京都品川区北品川6丁目7番35号 |
| 氏 名 | ソニー株式会社 |